Information Assurance Punitive aspects of AR 25-2

In the event that any supervisor intends to tal administrative action against any employee (U.S. service member, civilian, LN), they shou with the JAG office prior to taking any action

AR 25-2

INFORMATION ASSURANCE

- AR 25-2, paragraph 1-1 j makes various provisions of AR 25-2 punitive in nature.
- Military could be subject to Article 92 of the UCMJ.
- DA Civilians subject to administrative punishment
- Contractors subject to contract remedies.

AR 25-2 Prohibitions

- **Paragraphs 3-2 and 3-3. Failure to perform the listed duties if assigned to listed position.**
- **Paragraph 4-6. Failure to comply with software security controls. (e.g. violating baselines or using shareware/freeware)**
- **Paragraph 4-7. Failure to comply with database management directives and controls. (e.g. unauthorized access)**
- **Paragraph 4-10. Failure to comply with personnel access restrictions. (e.g. use of maintenance personnel or use of data recovery services)**

AR 25-2 Prohibitions

- **Paragraph 4-11. Failure to comply with security safeguards. (e.g physical security)**
- **Paragraph 4-12. Failure to comply with password controls.**
- **Paragraph 4-13. Improper release of information concerning information system infrastructure architecture. (e.g public access to FOUO material)**
- **Paragraph 4-16. Failure to comply with information systems media protection requirements. (e.g. protect classified material)**

AR 25-2 Prohibitions

- Paragraph 4-17. Failure to comply with classification labeling and marking requirements.
- Paragraph 4-18. Failure to properly clear, purge, destroy, sanitize, or otherwise dispose of media.
- Paragraph 4-20. Failure to comply with network security requirements. (e.g. use of commercial networks, forward of official mail to civilian email systems)
- Paragraphs 4-21and 4-22. Failure to comply with incident and intrusion reporting requirements.

AR 25-2 Requirements

- **Paragraph 4-23. Failure to comply with requirements concerning compromised systems.**
- **Paragraph 4-25. Failure to follow IAVA compliance reporting requirements.**
- **Paragraph 4-30. Violations of restrictions on employee and contractor owned information systems.**
- **Paragraph 6-1. Failure to comply with COMSEC requirements.**

AR 25-2 Requirements

- **Paragraph 6-2. Violation of the restrictions on protected distribution systems. (e.g inspection of and access to secure network boxes/pipes in unclassified areas)**
- **Paragraph 6-5. Violations of restrictions on telecommunications devices. (e.g. government or personal PDA's, cell phones, pagers, etc in secure areas)**

AR 25-2 Paragraph 4-5

- **Paragraph 4-5, including:**
- **Prohibited Activities to include JER prohibitions <u>plus</u>:**
- **File or music sharing covered as copyright infringements.**
- **Modify of system equipment or software, use for unintended purposes, introduction of malicious code or software, or adding unauthorized software such as instant messaging or peer to peer.**
- **Attempts to bypass security mechanisms**

AR 25-2, Paragraph 4-5

- Relocate or change IS equipment or the network connectivity of IS equipment without proper security authorization.
- Improperly disclose information on the system.
- Share personal accounts or passwords
- Disable or remove security devices.

AR 25-2 Paragraph 4-5

- Failure to comply with requirements concerning:
- Accreditation
- Access control
- Remote access and remote access servers
- Configuration Management requirements
- Data Integrity
- IA Product Acquisition
- Security Training and Awareness
- Warning Banners and Consent Procedures
- Virus Protection
- Mobile Code (e.g. viruses, spyware)
- Acceptable Use Policy
- Monitoring Networks